

AMENDMENT

Amendments to the Claims: Please replace all prior versions and listings of claims with the following listing of claims.

LISTING OF CLAIMS:

1. (Currently Amended) A method for detecting and preventing attacks directed at a target system, comprising:

receiving one or more packets originating from a source system, the received packets directed to the target system;

monitoring the received packets to identify one or more of the packets that include information associated with an attack signature, the attack signature associated with one or more previous attacks directed at the target system;

detecting an attack directed at the target system when one or more of the monitored packets include information associated with the attack signature;

creating an attack profile based on information related to the detected attack, wherein the attack profile includes information related to the monitored packets that include information associated with the attack signature;

blocking one or more of the monitored packets that include information associated with the attack signature profile from being transmitted to the target system; and

blocking one or more subsequently received packets from being transmitted to the target system when a severity of the detected attack exceeds a predetermined threshold, the subsequently blocked packets including one or more of packets originating from the source system or directed to the target system.

2. (Previously Presented) The method according to claim 1, wherein monitoring the packets includes determining at least one of identifying information or a type of communication associated with the monitored packets.

3. (Previously Presented) The method according to claim 2, wherein the identifying information includes at least one of a source Internet Protocol address, a source port number, a destination Internet Protocol address, or a destination port number.
4. (Previously Presented) The method according to claim 2, wherein the type of communication includes at least one of File Transfer Protocol, Simple Mail Transfer Protocol, Telnet, Domain Name System, Windows Internet Name System, HyperText Transfer Protocol, Traceroute, instant messaging, or chat.
5. (Previously Presented) The method according to claim 1, wherein monitoring the packets includes using Transmission Control Protocol/Internet Protocol at an application layer.
6. (Previously Presented) The method according to claim 1, further comprising determining the severity of the detected attack based on at least one of a frequency of the previous attacks, a type of communication used in the previous attacks, an amount of bandwidth usage associated with the previous attacks, or a volume of the received packets.
7. (Previously Presented) The method according to claim 1, wherein blocking the packets from being transmitted to the target system includes instructing at least one of a router, a hub, a server, or a firewall to disable a communication channel.
8. (Previously Presented) The method according to claim 1, further comprising notifying the source system that the attack has been detected and that a block was placed on packets received from the source system.
9. (Previously Presented) The method according to claim 1, wherein the subsequently received packets are blocked from being transmitted to the target system for a predetermined amount of time.

10. (Currently Amended) A system for protecting a computer network, comprising at least one computer readable medium associated with a device coupled to the network, the computer readable medium including:

a detection module that receives attack signatures associated with one or more previous attacks directed at a target device, monitors one or more received packets to identify one or more of the packets that include information associated with the attack signatures, and detects an attack directed at the target device when one or more of the packets include information associated with the attack signatures;

a scanning module that determines a severity of the detected attack directed at the target device; and

a log creating module that creates an attack profile based on information related to the detected attack, wherein the attack profile includes information related to the monitored packets that include information associated with the attack signature;

a blocking module that identifies a source of the packets that include information associated with the detected attack ~~signatures~~, instructs at least one device to block one or more of the monitored packets that include information associated with the attack ~~signatures~~ profile from being transmitted to the target device, and instructs the at least one device to block one or more subsequently received packets from being transmitted to the target device when the severity of the detected attack exceeds a predetermined threshold, the subsequently blocked packets including one or more of packets originating from the source or directed to the target device.

11. (Currently Amended) The system according to claim 10, wherein the ~~computer readable medium further includes a log creating module that creates a log record~~ of the packets identified as including the information ~~associated with~~ related to the detected attack ~~signatures~~.

12. (Previously Presented) The system according to claim 10, wherein the detection module monitors the received packets by determining at least one of identifying information or a type of communication associated with the monitored packets.

13. (Previously Presented) The system according to claim 10, wherein the scanning module determines the severity of the detected attack based on at least one of a frequency of the previous attacks, a type of communication used in the previous attacks, an amount of bandwidth usage associated with the previous attacks, or a volume of the received packets.

14. (Previously Presented) The system according to claim 10, wherein the blocking module blocks the packets from being transmitted to the target device by instructing at least one of a router, a hub, a server, or a firewall to disable a communication channel.

15. (Previously Presented) The system according to claim 14, wherein the blocking module blocks the packets from being transmitted to the target device for a predetermined amount of time.

16. (Currently Amended) A computer readable medium containing computer executable instructions for detecting and preventing attacks directed at a target system, the computer executable instructions operable to:

- receive one or more packets originating from a source system, the received packets directed to the target system;

- monitor the received packets to identify one or more of the packets that include information associated with an attack signature, the attack signature associated with one or more previous attacks directed at the target system;

- detect an attack directed at the target system when one or more of the monitored packets include information associated with the attack signature;

create an attack profile based on information related to the detected attack, wherein the attack profile includes information related to the monitored packets that include information associated with the attack signature;

block one or more of the monitored packets that include information associated with the attack signature profile from being transmitted to the target system; and

block one or more subsequently received packets from being transmitted to the target system when a severity of the detected attack exceeds a predetermined threshold, the subsequently blocked packets including one or more of packets originating from the source system or directed to the target system.

17. (Previously Presented) The computer readable medium according to claim 16, wherein the received packets are monitored transparently in real time.

18. (Previously Presented) The computer readable medium according to claim 16, wherein the received packets are monitored after being stored in a storage buffer.

19. (Previously Presented) The computer readable medium according to claim 16, the instructions further operable to determine the severity of the detected attack based on at least one of a frequency of the previous attacks, a type of communication used in the previous attacks, an amount of bandwidth usage associated with the previous attacks, or a volume of the received packets.

20. (Previously Presented) The computer readable medium according to claim 16, the instructions operable to block the packets from being transmitted to the target system by instructing at least one of a router, a hub, a server, or a firewall to disable a communication channel.

21. (Previously Presented) The computer readable medium according to claim 16, the instructions further operable to notify the source system that the attack has been detected and that a block was placed on packets received from the source system.

22. (Previously Presented) The computer readable medium according to claim 16, the instructions operable to block the packets from being transmitted to the target system for a predetermined amount of time.

23. (Currently Amended) A computer system configured for detecting and preventing attacks directed at target devices, comprising:

at least one terminal device;

at least one server coupled to a computer network and to the terminal device, the server operable to monitor packets directed to the terminal device, the server having one or more modules, including:

a detection module that receives attack signatures associated with one or more previous attacks directed at the terminal device, monitors one or more received packets to identify one or more of the packets that include information associated with the attack signatures, and detects an attack directed at the terminal device when one or more of the packets include information associated with the attack signatures;

a log creating module that creates an attack profile based on information related to the detected attack, wherein the attack profile includes information related to the monitored packets that include information associated with the attack signature;

a scanning module that determines a severity of the detected attack directed at the terminal device; and

a blocking module that identifies a source of the packets that include information associated with the detected attack signatures, instructs at least one switching device to block one or more of the monitored packets that include information associated with the attack signatures profile from being transmitted to the terminal device, and instructs the at least one switching device to block one or more

subsequently received packets from being transmitted to the terminal device when the severity of the detected attack exceeds a predetermined threshold, the subsequently blocked packets including one or more of packets originating from the source or directed to the terminal device.

24. (Currently Amended) The computer system according to claim 23, wherein the server ~~further includes a log creating module that creates a log record of the packets identified as including the information associated with related to the detected attack signatures.~~

25. (Previously Presented) The computer system according to claim 23, further comprising a database coupled to the server.

26. (Previously Presented) The computer system according to claim 23, wherein the detection module monitors the received packets by determining at least one of identifying information or a type of communication associated with the monitored packets.

27. (Previously Presented) The computer system according to claim 23, wherein the scanning module determines the severity of the detected attack based on at least one of a frequency of the previous attacks, a type of communication used in the previous attacks, an amount of bandwidth usage associated with the previous attacks, or a volume of the received packets.

28. (Previously Presented) The computer system according to claim 23, wherein the blocking module blocks data packets from being transmitted to the terminal device by instructing at least one of a router, a hub, a server, or a firewall to disable a communication channel.

29. (Previously Presented) The computer system according to claim 23, wherein the blocking module blocks the packets from being transmitted to the terminal device for a predetermined amount of time.

30. (Previously Presented) The computer system according to claim 23, the server further operable to issue an alert to inform an administrator of the network of the detected attack directed at the terminal device.

31. (Previously Presented) The method according to claim 3, the subsequently blocked packets including packets associated with one or more of the source Internet Protocol address, the source port number, the destination Internet Protocol address, or the destination port number.

32. (New) The method according to claim 1, wherein the attack profile includes information related to suspected and/or confirmed attacks directed at the target system.

33. (New) The system according to claim 10, wherein the attack profile includes information related to suspected and/or confirmed attacks directed at the target system.

34. (New) The computer readable medium according to claim 16, wherein the attack profile includes information related to suspected and/or confirmed attacks directed at the target system.

35. (New) The computer system according to claim 23, wherein the attack profile includes information related to suspected and/or confirmed attacks directed at the target system.